Security Quickie 1-31-03: Proactive Security

As most of you know, last weekend's SQL Slammer worm dramatically affected many businesses around the world. It slowed down or swamped many systems with SQL traffic, creating a huge denial of service attack on many Internet systems. Financial companies like Countrywide Financial Corp., American Express, and Bank of America couldn't serve their customers needs because of the worm. Even the largest ISP in South Korea was brought to its knees for a time. Yet the State of Iowa was largely unaffected by this. Why? Were we just lucky?

Nope. We were unaffected because the State of Iowa takes a proactive security stance. A patch for the SQL flaw was announced about a half-year ago, and since that time state administrators patched our existing systems. New systems go through configuration lock-downs, which include securing the services that servers host and eliminating services they don't. Administrators check out vulnerability alerts and apply patches because they know exploits are only a matter of time. Personnel follow security procedures, like using only the services they need. Everybody learns and applies their knowledge to keep themselves and the state secure. In other words, state employees have been able to act before incidents occur to either minimize incident effects or eliminate their possibility.

The State of Iowa's proactive stance toward security has likely minimized or eliminated the effects of many other incidents as well. By using proper policies, products, and behaviors all of us have limited viral and worm infections, loss of confidential information, and loss of services that citizens depend on us for. It comes down to having knowledgeable staff and good secure behavior – and believe it or not, we've got both. Congrats, everyone.